CLAIMS

What is claimed is:

1. A method for managing security information comprising the steps of:

receiving raw events from one or more data sources;

classifying the raw events;

storing the raw events;

assigning a ranking to each raw event;

identifying relationships between two or more raw events;

in response to identifying any relationships between two or more raw events, generating a mature correlation event message; and

displaying one or more mature correlation event messages on a console that describe relationships between raw events.

2. The method of claim 1, wherein each raw event comprises suspicious computer activity detected by one of an automated system and human observation.

3. The method of claim 1, wherein the step of receiving raw events from one or more data sources further comprises the step of receiving real-time raw events from one of intrusion detection system, a detector within an intrusion detection system, and a firewall.

4. The method of claim 1, wherein the step of receiving raw events from one or more data sources further comprises the step of receiving raw events from one of a file and database.

5. The method of claim 1, wherein the step of classifying the raw events further comprises the steps of:

identifying an event type parameter for each raw event;

comparing the event type parameter with an event type category of a list; and assigning each raw event to a corresponding event type category in the list.

6. The method of claim 1, wherein the step of assigning a ranking to each raw event further comprises the steps of:

comparing parameters of each raw event with information in a database; and

assigning additional parameters to each raw event relating to the environment of the raw event.

7. The method of claim 6, wherein the additional parameters comprise one of a priority status, a vulnerability status, a historical frequency value, a source zone value, a destination zone value, a detector zone value, and a text string.

8. The method of claim 1, wherein the step of assigning a ranking to each raw event further comprises the steps of:

identifying a priority status parameter of a raw event;

comparing each raw event to information contained in a context database;

changing the priority status parameter of a respective raw event if a match occurs in response to the comparison step; and

leaving the priority status in tact if a match does not occur in response to the comparison step.

9. The method of claim 1, wherein the step of identifying relationships between two or more raw events further comprises the steps of:

associating each raw event with a rule which corresponds with a type parameter of a raw event; and

applying one or more rules to groups of raw events having the same type parameter; and

determining if a computer attack or security breach has occurred based upon successful application of a rule.

10. The method of claim 1, wherein the step of storing raw events further comprises the step of storing each raw event in a high speed memory device comprising random access memory (RAM).

11. The method of claim 1, further comprising the step of determining the intent of a computer attack based upon the type of mature correlation event generated.

12. The method of claim 1, further comprising the steps of:

creating a memory management list;

identifying a time stamp for each raw event; and

adding each raw event to the memory management list.

13. The method of claim 1, further comprising the step of creating a raw event tracking index that identifies one or more software components that are monitoring one or more raw events.

14. A method for determining relationships between two or more computer events, comprising the steps of:

receiving a plurality of raw events having a first set of parameters;

creating raw event storage areas based upon information received from a raw event classification database;

storing each event in an event storage area based upon an event type parameter;

comparing each raw event to data contained in a context database;

adjusting a priority parameter or leaving the priority parameter in tact for each raw event in response to the comparison to the context database;

associate each raw event with a correlation event;

applying one or more rules to each event based upon the correlation event association; and

generating a mature correlation event message in response to a successful application of a rule.

15. The method of claim 14, wherein each raw event comprises suspicious computer activity detected by one of an automated system and human observation.

16. The method of claim 14, wherein the context database comprises any one of vulnerability values, computer event frequency values, and source and destination zone values.

17. The method of claim 14, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how a raw event may impact one or more target computers, how many target computers that may be affected by a raw event, and how respective raw events gain access to one or more target computers.

18. A security management system comprising:

a plurality of data sources;

an event collector linked to the plurality of data sources;

a fusion engine linked to the event collector, said fusion engine identifying relationships between two or more raw events generated by the data sources; and

a console linked to the event collector for displaying any output generated by the fusion engine.

19. The security management system of claim 18, further comprising a detector, the detector running in a kernel mode of a computer and the fusion engine running in a user mode of the computer.

20. The security management system of claim 18, further comprising a detector chip, and the fusion engine comprising software running on a computer.

21. The security management system of claim 18, further comprising a detector board, and the fusion engine comprising software running on a computer.

22. A fusion engine comprising:

a controller;

an event reader for receiving raw events;

a classifier linked to the event reader for classifying the received raw events;

a raw event classification database linked to the classifier;

a context based risk-adjustment processor linked to the classifier, for adjusting priorities of raw events;

a context database linked to the context based risk-adjustment processor; and

a rule database, for determining if relationships exist between two or more events.

23. The fusion engine of claim 22, further comprising an event reporter, a mature event list, a memory management list, and a raw event tracking index .

24. The fusion engine of claim 22, wherein the context database comprises any one of vulnerability values, computer event frequency values, and source and destination zone values.

25. The fusion engine of claim 22, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how a raw event may impact one or more target computers, how many target computers that may be affected by a raw event, and how respective raw events gain access to one or more target computers.